DSB Summer Study Report on

Strategic Surprise

July 2015

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
DSB Summer Study Report on Strategic Surprise	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Science Board (DSB),The Pentagon ,OUSD(AT&L) Room 3B888A,Washington,DC,20310**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**22**	

This page intentionally blank

REPORT OF THE DEFENSE SCIENCE BOARD

STUDY ON

Strategic Surprise

July 2015

Office of the Under Secretary of Defense
for Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense (DoD). The Defense Science Board Study on Strategic Surprise completed its information-gathering in August 2014. The report was cleared for open publication by the DoD Office of Security Review on September 29, 2015.

This report is unclassified and cleared for public release.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE BOARD

February 26, 2015

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY & LOGISTICS

SUBJECT: Final Report of the Defense Science Board (DSB) Summer Study on Strategic Surprise

I am pleased to forward the final report of the DSB Summer Study on Strategic Surprise. This report offers important recommendations on how the Department can prevent regrets in 2024 by acting now to counter potential adversary actions in the next decade.

The study focused on potential regrets in eight domains that include: countering nuclear proliferation; ballistic and cruise missile defense; space security; undersea warfare; cyber; communications and positioning, navigation, and timing (PNT); counterintelligence; and logistics resilience. This report provides recommendations to detect and protect against threats, develop new capabilities, and strengthen current capabilities to hedge against strategic surprise.

The study also provides thoughts on how to create strategic surprise for our adversaries in the next decade.

I fully endorse all of the recommendations contained in this report and urge their careful consideration and soonest adoption.

Craig Fields
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE BOARD

February 26, 2015

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

Subject: Final Report of the Defense Science Board 2012 Summer Study on Strategic Surprise

The final report of the Defense Science Board 2014 Summer Study on Strategic Surprise is attached. In accordance with its charter, the study reviewed how information about a potential adversary may lead to changing current Department priorities and what the possible actions and hedges against those changing priorities may be. The study considered what actions, if not taken by the Department, might lead to potential regrets in 2024. They study also reviewed possible actions and hedges against changing priorities.

The study focused on potential regrets in eight areas and provides recommendations to avoid strategic surprise in those eight domains. The domains include:

- Countering Nuclear Proliferation
- Ballistic and Cruise Missile Defense
- Space Security
- Undersea Warfare
- Cyber
- Communications and Positioning, Navigation, and Timing (PNT)
- Counterintelligence
- Logistics Resilience

To determine the potential regrets in 2024, the study focused on the likelihood of the regret occurring and the consequences if it does occur. In providing recommendations, the study focused on whether there are affordable and timely ideas to prevent the undesired outcome, and also whether the Department is already taking action toward this end.

In each of the domains, the study provides the current trends, challenges, and threats the Department faces. These trends, challenges, and threats are each followed by specific regrets in 2024 to the Department with domain-specific strategies and recommendations. Given the current budget environment, implementing all of these recommendations will necessitate a realignment of resources. In many cases, the strategies provide a way forward by providing the Department with new frameworks for current initiatives.

The study also encourages the Department to consider several cross-cutting imperatives to address strategic surprise. These include moving "left of launch" and rebalancing current U.S. capabilities to provide options for going on the offense through early prepositioning of assets. To accomplish this, each domain will require a shift to gather smarter and earlier deep intelligence. The domains impacted the most by earlier intelligence will be countering nuclear proliferation and ballistic and cruise missile defense. Across all domains, the proliferation of unmanned systems that work on their own as well as in concert with manned systems will change the Department's capability to respond to conflict. In order to accomplish these shifts, the Department must accelerate research and development and adopt autonomous systems in as many areas as possible to improve speed and costs.

Finally, the report provides thoughts on how to create strategic surprise for our adversaries in the next decade. Expanding the use of surprise and war reserves can be accomplished by leveraging existing systems for new missions through new concepts of operation and software. Rethinking combined weapons effects among conventional, space, undersea, cyber, and nuclear will provide the Department with new capabilities to face new threats. Finally, the study believes that counterintelligence must be enhanced with urgency while speeding up our own experimentation, development, and fielding of new capabilities.

The study believes that all of the recommendations contained in this report are critical for ensuring the Department experiences as few regrets as possible in 2024.

Mr. Vincent Vitto
Co-Chairman

Dr. David Whelan
Co-Chairman

In April 2014, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) directed the Defense Science Board (DSB) to conduct an abbreviated study to "consider what information about any potential adversary may not be sufficiently acted upon in the decades to come that will lead to regrets in 2024; and in broad terms what those actions and hedges against changing priorities might be."[1]

The areas for consideration included: maturation of science and technology; development of new weapons and weapons concepts including weapons of mass destruction; emergence of new operational concepts and rules of engagement; different potential adversaries and different kinds of potential adversaries; changing alliances among potential adversaries and changing relationships between the United States and its allies; broad global trends such as demographic shifts, geopolitical changes, resource constraints, or climate change; evolving priorities for national security objectives; and foreign policy goals.

To address this charge in a timely manner, the DSB called primarily on the expertise of members of the Board. The study met from June through August 2014 to explore potential changes for Department of Defense priorities as well as possible actions and hedges to strategic surprise and avoid potential regrets in 2024.

A Changing Context for Operations

The study explored current and future operational contexts. The study defined "strategic surprise" as an event for which the United States is not adequately prepared and that may result in very high cost. It was assumed that such an event will inevitably occur in today's complex and rapidly changing world.

Since the end of the cold War, the U.S. and its allies have engaged in four armed conflicts against adversaries who did not significantly threaten the Department of Defense's overall military capability. These conflicts include Operation Desert Storm in 1991, the Bosnian War in 1993, Operation Enduring Freedom in 2001, and Operation Iraqi Freedom in 2003. Throughout these conflicts, U.S. forces were supported by a secure homeland and supremacy in air, space, ground, and maritime capabilities. U.S. forces also had secure command, control, communications, computers, intelligence, surveillance and reconnaissance (C41SR) capabilities and dominance in the electromagnetic spectrum.

Despite the dominance that the U.S. retains in many areas, potential adversaries are taking actions to level the playing field. Today's world is full of challenges and many ripe opportunities exist for adversaries to create surprise. Now the U.S. military must prepare for a wider range of highly capable adversaries. These adversaries now have access to rapid advances that have been made in science and technology, many of which have been accomplished outside of any government organization. Global diffusion of these advanced technologies is threatening U.S. technological dominance and empowering nontraditional individuals and groups that are now able to afford entry. These changing conditions increasingly compel DoD to become an exploiter, rather than a creator, of technology in the future.

1 Terms of Reference for the Defense Science Board 2014 Summer Study on Strategic Surprise, April 7, 2014.

DoD continues to plan and acquire systems focused on countering near-peer or regional adversary kinetic capabilities without addressing threats to our critical warfighting infrastructure. In the future, the U.S. military must prepare for direct threats to the U.S. homeland and area denial by capable adversaries. Military forces must also prepare for nuclear, biological, chemical use as well as cyber attacks on military and critical infrastructure. Major threats to U.S. air, space, and maritime platforms are likely, and will include extensive adversary electronic warfare on surveillance, communications, and GPS systems. Most pervasively, the U.S. must understand and be prepared to counter technology diffusion to large and small global actors.

Potential Regrets in 2024

The study assessed potential outcomes that the U.S. and DoD may regret in 2024. The study members prioritized and filtered potential regrettable outcomes through the following questions:

1. What are the consequences of a regrettable outcome in 2024?
2. What is the likelihood of it happening?
3. Are there good ideas to prevent it from happening? Are any ideas affordable and timely?
4. Is DoD already doing something that might keep it from happening?

The study considered a wide range of topics. The maturation of science and technology and the need for rapid development and deployment of new capabilities were ubiquitous and influenced all of the specific topics addressed by the study.

The eight focus areas discussed in this report, are as follows:

- Countering nuclear proliferation
- Securing ballistic and cruise missile defense
- Improving space security
- Advancing undersea warfare
- Defending against cyber attacks
- Protecting military communications and PNT
- Developing effective counterintelligence
- Establishing resilient logistics systems

Strategies

Some of the strategic surprises the study considered were an attack on the homeland using WMDs. Such an attack could be enabled by nuclear, chemical, and biological weapons fabricated in a garage shop, and the DoD would regret their failure to use big data and cyber capabilities to gain possible network discovery and early warning. Similarly, a kinetic attack on the homeland could come from a cruise missile attack by the use of containerized weaponry, or an attack on ports, bases, or shipping from prepositioned autonomous undersea assets. One of the most disruptive surprises could

be a major cyber attack that changes the American way of life, such as a cyber attack on major U.S. infrastructure or a kinetic attack on transoceanic cables or major data centers.

To find ways to hedge against these and similar surprises—and to avoid regretting actions or lack of action taken today—the study evaluated several key mission and enterprise areas. Some of the key elements of the strategies proposed in each area are summarized here.

To maintain information dominance, DoD must make cyber a strategic capability to support every mission. One vital example is in countering nuclear proliferation, where DoD must strengthen intelligence approaches through big data analysis of enhanced cyber exploitation and integrating multiple intelligence sources to achieve early warning capabilities. DoD must also ensure that a critically important subset of DoD conventional forces are cyber trustworthy.

To provide secure ballistic and cruise missile defense, DoD will need to develop capabilities that allow its forces to move "left of launch" and attack the kill chain. To improve security for all space assets, DoD will need to improve space situational awareness through stronger threat assessments and attribution. DoD must also accelerate their transition from space situational awareness to space control. Finally, to advance undersea warfare capabilities, DoD must accelerate current programs and fund new initiatives that focus on the development of multimission networks for smart UUVs.

The key strategies proposed for military communications and PNT are to develop and deploy terminals that improve the performance of communications systems in a jammed environment. A second important step will be to accelerate the programs for improving GPS resilience.

To develop effective counterintelligence, new commercial encryption techniques will be needed to protect information. The use of big data analytics could allow DoD to track anomalies in the behaviors of cleared personnel in order to thwart the insider threat. Ensuring a resilient logistics system is also critical. To do this, DoD must protect the supply chain from attack, and must also protect U.S. forces from attackers that plot penetrate the supply chain. An important measure to ensure logistics systems are resilient is to significantly strengthen the information technology infrastructure of the U.S. Transportation Command (USTRANSCOM).

Each of these proposed strategies provides a starting point for protecting DoD and the U.S. against strategic surprise and potential regrets in 2024. The areas discussed specifically in the report are only a few of those that may present DoD with strategic surprise, and could cause serious regrets by 2024.

Recommendations

A summary of the specific recommendations for each of the eight domains are presented below:

Countering Nuclear Proliferation

Recommendation 1	**Developing early proliferation detection**

The Defense Threat Reduction Agency (DTRA), National Nuclear Security Agency (NNSA), the Intelligence Community (IC), and the Department of Homeland Security (DHS) should create an early warning capability for proliferation detection sensitive to the new technical pathways technology is now enabling.

- DTRA and the intelligence community could begin by expanding the current program in counter-WMD global awareness to support an early warning function. Integration of different intelligence sources will also be critical to this effort using big data techniques to address the expanded signatures associated with small or nascent programs. The Defense Advanced Research Projects Agency (DARPA) currently has the capability to advance this effort and to address the likely deception and denial complications. Finally, the feasibility, signatures, and impacts of new pathways to nuclear acquisition deserve exploration, potentially as an expansion of current programs in NNSA.

Recommendation 2	**Developing concepts for combined weapons operations**

The Deputy Secretary of Defense should charter a working group of policy, operational, and technical experts to assess how the U.S. could evolve its strategy and doctrine for creating new nonnuclear options for deterrence.

Recommendation 3	**Ensuring forces can fight through a nuclear event**

Secretary of Defense should direct the regional Combatant Commanders to identify mission-critical capabilities for conventional force operations to achieve mission success in a nuclear environment; and direct the Military Services to assure the operational integrity of those critical capabilities.

Ballistic and Cruise Missile Defense

The Department of Defense should undertake efforts to balance its strategy and investments to protect critical U.S. assets against advanced weapon systems.

Recommendation 4	**Taking a holistic view of missile defense**

DoD should take a holistic view of potential U.S. measures to defend against ballistic and cruise missiles ranging from active defenses to steps taken prior to weapon launch.

Recommendation 5	**Considering the entire adversary enterprise to balance the defense portfolio**

DoD should consider the entire enterprise required for an adversary to deliver a capable ballistic or cruise weapon when balancing the defense portfolio.

Recommendation 6	**Considering approaches to disrupt adversary weapon systems**

DoD should consider approaches with the potential to disrupt adversary weapon systems.

Space Security

Recommendation 7	Improving space surveillance architectures

The Department should improve space surveillance architectures through the following three initiatives.

- United States Strategic Command (USSTRATCOM) implement current planned space situational awareness (SSA) materiel and non-materiel solutions, including programs of record, courses of actions, and international sharing agreements.
- The Executive Agent for Space (EA4S) and the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) develop and field an integrated SSA and space architectures aligned with Battle Management Command, Control, and Communications (BMC3) requirements.
- The Office of the Deputy Assistant Secretary of Defense for Space Policy (ODASD(SP)) and USSTRATCOM leverage commercial and allied space surveillance capabilities, products, and services.

Recommendation 8	Enabling stronger space offense

The Department should assess current policy and develop a strategy to enhance space resilience to enable stronger space offense through the following two initiatives.

- USD(AT&L) and the Secretary of the Air Force should maintain capabilities to support the space control mission.
- USD(AT&L) and OUSD(I) develop and enhance innovative analytic tools and techniques to exploit and share traditional and nontraditional sources of information and understanding on foreign space-related activities.

Recommendation 9	Enhancing space security

The Department should enhance space security through the following three initiatives.

- ODASD(SP) and EA4S focus on achieving interoperable space enterprise architecture comprised of national, commercial, allied, and non-space capabilities.
- USD(AT&L) and the Secretary of the Air Force research and field tech-forward defensive options that are both passive and active.
- USD(AT&L) and the Secretary of the Air Force develop rapid reconstitution capability.

Undersea Warfare

Recommendation 10	Developing an integrated approach

The U.S. Navy should develop a more integrated approach for developing and using undersea warfare (USW) systems.

- The approach should address the projected threat and embrace options to transition capabilities to unmanned undersea systems and distributed sensors. The approach should be driven by OSD and Navy identification and characterization of the missions and desired effects that will migrate to the undersea domain and include new missions enabled by the undersea sanctuary.

Recommendation 11 Disrupting and imposing high-costs on potential adversaries

The U.S. Navy should emphasize a low-cost, effects-based USW strategy that can disrupt and impose high costs on potential adversaries.

- This goal can be accomplished by using coordinated UUVs and distributed sensors working in concert with manned platforms to deliver kinetic attack and to disrupt and confuse adversaries, which will require an increased emphasis on accelerating off-board capabilities, strategy development and enhanced command, control and communications. The focus should be on exploiting available undersea technology, commercial manufacturing, and low-cost prototype systems to ensure an affordable path to rapid full-scale deployment.

Recommendation 12 Protecting critical undersea infrastructure

OSD and the Navy should develop new concepts to protect critical undersea infrastructure.

- U.S. defensive posture needs to include both defense of undersea infrastructure and response to a re-emergent threat to CONUS. Given limitations on the numbers of manned platforms and the large ocean areas, new concepts beyond current platform-oriented solutions will be required.

Cyber

Recommendation 13 Ensuring the trustworthiness and integrity of critical systems

Department of Defense (DoD) should ensure that a critically important subset of DoD conventional forces is cyber trustworthy. These forces must be significantly hardened against cyber attack as well as be able to operate disconnected from any network. To be effective, these forces will have the capability to perform system integrity validation checks on all information systems before and during a conflict.

- USD(AT&L) should implement security best practices into acquisition and procurement processes.
  - These best practices should include such approaches as implementing heterogeneous architectures that increase the cost for adversaries to compromise. Similarly, making small changes to systems more frequently is a practice that will increase difficulty for adversaries to compromise them.

  - Other approaches are to add small amounts of government-off-the-shelf (GOTS) technology to commercial-off-the-shelf (COTS) technology, thereby forcing adversaries to write DoD-specific exploits. One last example of such a practice is to obfuscate the information technology hardware and software that DoD buys in order to force adversaries to query DoD systems thereby creating another opportunity to detect their activities.
- The Chairman of the Joint Chiefs of Staff (CJCS) should lead a demonstration of system integrity validation methods and DoD-specific security scoring systems.
  - DoD should create pilot programs to assess current technologies and methods for performing system integrity validation. The programs should call for differing approaches including physical memory-based, system introspection, and hardware assisted.
  - The methods needed for enterprise information technology, command and control, and weapons systems may be accomplished by DoD developing methods to operate partially-trusted systems or recover systems to a trusted state based on security scoring and the mission criticality of the system.

Recommendation 14 Making cyber a strategic capability

Department of Defense should elevate offensive and defensive cyber operations to a strategic capability.

- The Department should treat cyber as a military capability of the highest priority. To accomplish this, the Services must hire additional personnel, provide training, and invest in research and development to support cyber as a strategic capability.
- United States Cyber Command (USCYBERCOM) should develop operational procedures for utilizing cyber capabilities across a broad spectrum of activities and actions. Operators must train and exercise and those exercises must be realistic with accountability for correcting negative outcomes. To be most effective these realistic exercises must include not only cyber-only exercises but also working with other conventional forces in a combined arms mode. In addition, USCYBERCOM needs to ensure the availability of the required modeling and simulation capabilities and test facilities.

Recommendation 15 Leveraging the Internet of Things

Department of Defense should create a working group to continuously monitor and influence the standards and cyber security facets of emerging Internet of Things (IoT) technology.

- DARPA should create pilot programs to develop DoD-specific technologies and capabilities to monitor, access, manage, and disrupt the IoT.
- DARPA should create pilot programs to create and evaluate technologies and capabilities to utilize the IoT as a large-scale ISR environment as well as to undermine an adversaries' ability to do the same.

Communications and Positioning, Navigation and Timing

Recommendation 16 Ensuring a robust communications and PNT infrastructure

The Department of Defense should ensure a robust communications and PNT infrastructure and establish updated concepts of operations (CONOPS) to address projected threats. The study recommends this be accomplished through the following five initiatives.

- The Joint Staff, J6, should develop joint and multi-national communications and PNT architecture, roadmap, and investment plans and re-visit current topologies, equipment buys, deployment strategies, and schedules. Specifically, the deployment of Advance Extremely High Frequency (AEHF) terminals to critical nodes and developing anti-jam improvements to HAVEQUICK and Link-16 need attention. The J6 should also advocate for development and deployment of adaptive anti-jam modems for commercial satellite communications.
- USD(AT&L) and the Services should implement the recommendations of the GPS Enterprise Modernization Analysis of Alternatives that was approved by the Joint Requirements Oversight Council (JROC) in January 2013. In addition, the Department must support advanced technologies and concepts that will extend and augment GPS performance.
- The J6 should plan a regular series of training and exercise scenarios with realistic EW environments or ensure realistic environments are considered in currently planned exercises. This will stress the architecture and evolve it in real time. It will also mitigate future surprises and prepare the warfighter to operate in disadvantaged or denied environments.
- USD(AT&L) should establish a joint working group with the Military Services, DARPA, and the defense laboratories to identify and propose hybrid solutions to increase resilience. An initial focus should be on offensive electronic attack strategies to ensure high-integrity communications and PNT. Additional focus areas should include communications and electro-optic technologies for assisted PNT and multistatic communications to assist electromagnetic spectrum situational awareness.
- ASD(R&E) should reassess and focus S&T investment for satellite communications in areas lacking commercial investment. Investment areas include enhancing low probability of intercept (LPI) and low probability of detection (LPD) utilizing time, frequency and spatial diversity; protecting against the effects of electromagnetic pulse (EMP) weapons; producing atomic clocks and inertial measurement units (IMUs) at tactical prices; creating bandwidth aware applications; and designing appliqués that leverage commercial infrastructure.

Recommendation 17 Pursuing alternative contractual opportunities

DoD should designate and empower USD{AT&L) as a single source authority to implement better buying practices for commercial satellite communications.

- The Defense Business Board recommendations should be implemented to include exercising more capital leases for long-term needs; increased public-private collaboration for more

economical solutions like hosted platforms; and improved governance of communications systems.

– A program similar to the Civil Reserve Air Fleet (CRAF) program should be established for satellite communications with potential extensions to other modes of communication.

Recommendation 18	**Moving beyond the current spectrum strategy toward full sharing of communications spectrum across current commercial and military boundaries**

The study recommends the following two initiatives for DoD to implement to move beyond the current spectrum strategy.

– Defense Information Systems Agency (DISA) and DoD Chief Information Officer (CIO) evolve and update DoD spectrum strategy to fully leverage cognitive radio capabilities and lead changes and seek new allocations at World Radio Conference to enable spectrum sharing in selected bands.

– USD(ATL) incorporate spectrum synchronization review as part of milestone decision processes to better synchronize offensive, e.g., EW and defensive spectrum capabilities for situational awareness, protection, and attack.

Counterintelligence

Recommendation 19	**Utilizing available technology to protect critical information**

The Department of Defense should examine implementation of encryption techniques where the key is escrowed on the network rather than with the user.

– Limiting encryption techniques that are allowed to be utilized can help to ensure transparency for counterintelligence. Commercial technologies developed for digital rights management and securing sensitive information in the financial industry may prove useful for security management. For example, sensitive data may be automatically identified by content and context, and can be flagged when being exported from the network.

Recommendation 20	**Employing technology to continuously monitor secured personnel**

All defense information systems should continuously monitor cleared personnel with sensitive accesses.

– Continuous monitoring can be accomplished through the use of big data and creative analytics that combine physical and cyber security information with personnel security information. Insider actions often generate suspicious indicators in multiple and organizationally separate domains-physical, personnel, and cyber security. The use of big data and creative analytics can be carefully tuned to the style and workflow of the particular organization and can help to audit for integrity as well as individual user legitimacy.

- Software that learns over time may also be used to increase detection and decrease false alarms.
- Leveraging more open source data is also a sound approach to maintain a more complete picture of personnel with sensitive accesses.

Logistics Resilience

Recommendation 21 **Protecting against an attack on the supply chain**

USD(AT&L) should strengthen supply chain resilience and agility.

- One method is to enhance threat awareness through intelligence and industry partnership. Another method is to increase the application of red teaming to better understand adversary actions and create countermeasures that can contribute to ensuring a more dynamic and unpredictable supply chain.
- Where supply chains are threatened by cyber attacks, DoD should increase cyber situational awareness, cyber information sharing, cyber deception and active cyber defenses to increase the resilience of supply chains to cyber attack. The DoD should also pursue public private partnerships that align government interests with commercial suppliers, acquiring war reserves or pursuing life of type contracts.

Recommendation 22 **Protecting against an attack via the supply chain**

Military Services should enhance forward operating base resilience.

- Approaches to accomplish this include prepositioning assets to overcome the tyranny of distance and time, fostering diversity of supply and suppliers to reduce single sources of failure, dispersing both bases and assets to reduce centers of gravity, and hardening not only supplies and supply chain but valuable weapon systems.
- Approaches may also include methods for rapid reconstitution of supplies, such as 3D printing or other affordable local means of production. Rapid response to surprise is an important dimension of logistics agility.

Summary

The overarching objectives of the 2014 Defense Science Board Summer Study on Strategic Surprise was to consider what information about any potential adversary may not be sufficiently acted upon in the decade to come that will lead to regrets in 2024; and in broad terms what those actions and hedges against changing priorities might be.

Some of the strategic surprises the study considered were an attack on the homeland using WMDs. Such an attack could be enabled by nuclear, chemical, and biological weapons fabricated in a garage shop, and the DoD would regret their failure to use big data and cyber capabilities to gain possible network discovery and early warning. Similarly, a kinetic attack on the homeland could come from a cruise missile attack by the use of containerized weaponry, or an attack on ports, bases, or shipping from prepositioned autonomous undersea assets. One of the most disruptive surprises could be a major cyber attack that changes the American way of life, such as a cyber attack on major U.S. infrastructure or a kinetic attack on transoceanic cables or major data centers.

To find ways to hedge against these and similar surprises—and to avoid regretting actions or lack of action taken today—the study evaluated several key mission and enterprise areas. Some of the key elements of the strategies proposed in each area are summarized here.

To maintain information dominance, DoD must make cyber a strategic capability to support every mission. One vital example is in countering nuclear proliferation, where DoD must strengthen intelligence approaches through big data analysis of enhanced cyber exploitation and integrating multiple intelligence sources to achieve early warning capabilities. DoD must also ensure that a critically important subset of DoD conventional forces are cyber trustworthy.

To provide secure ballistic and cruise missile, DoD will need to develop capabilities that allow its forces to move “left of launch” and attack the kill chain. To improve security for all space assets, DoD will need to improve space situational awareness through stronger threat assessments and attribution. The Department must also accelerate their transition from space situational awareness to space control. Finally, to advance undersea warfare capabilities, DoD must accelerate current programs and fund new initiatives that focus on the development of multimission networks for smart UUVs.

The key strategies proposed for military communications and PNT are to develop and deploy terminals that improve the performance of communications systems in a jammed environment. A second important step will be to accelerate the programs for improving GPS resilience.

To develop effective counterintelligence, new commercial encryption techniques will be needed to protect information. The use of big data analytics could allow DoD to track anomalies in the behaviors of cleared personnel in order to thwart the insider threat. Ensuring a resilient logistics system is also critical. To do this, DoD must protect the supply chain from attack, and must also protect U.S. forces from attackers that plot to penetrate the supply chain. An important measure to ensure logistics systems are resilient is to significantly strengthen USTRANSCOM’s information technology infrastructure.

The study developed a number of strategies and recommendations for the eight domains that were assessed. The study believes that each of these recommendations are critical for ensuring the

Department experiences as few regrets as possible over the next ten years. The study also recognizes that the Department faces serious resource limitations and some of the recommendations call for investments within the future year defense program. However, the majority of strategies and associated recommendations provide a strategic framework that will allow the Department to address emerging threats and potential regrets with a methodology going forward that is driven by both system performance and cost-benefit analysis.

Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

APR 07 2014

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board 2014 Summer Study on Strategic Surprise

The objective of the 2014 Defense Science Board Summer Study is to consider what information about any potential adversary may not be sufficiently acted upon in the decade to come that will lead to regrets in 2024; and in broad terms what those actions and hedges against changing priorities might be.

Considerations should include: maturation of science and technology; development of new weapons and weapons concepts including weapons of mass destruction; emergence of new operational concepts and rules of engagement; different potential adversaries and different kinds of potential adversaries; changing alliances among potential adversaries and changing relationships between the United States and its allies; broad global trends such as demographic shifts, geopolitical changes, resource constraints, or climate change; evolving priorities for national security objectives; and foreign policy goals.

I will sponsor the study. Mr. Vince Vitto and Dr. Dave Whelan will serve as Co-chairmen of the study. Mr. Brian Hughes will serve as Executive Secretary. Captain James CoBell, USN will serve as the Defense Science Board Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act" and Department of Defense (DoD) Directive 5105.04, the DoD Federal Advisory Committee Management Program. It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, U.S.C., section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Frank Kendall

Members of the Study

Study Chairs

Mr. Vincent Vitto	Private Consultant
Dr. David Whelan	The Boeing Company

Executive Secretary

Mr. Brian Hughes	OUSD (AT&L)

Members

Dr. Amy Alving	Private Consultant
Dr. Michael Anastasio	Los Alamos National Laboratory
Dr. Wanda Austin	Aerospace Corporation
Mr. Michael Bayer	Private Consultant
Mr. Frank Cappuccio	Cappuccio & Associates LLC
Mr. James Carlini	Private Consultant
Gen. Michael Carns (ret)	Private Consultant
Dr. Arup Chakraborty	MIT
Hon. David Chu	Institute for Defense Analyses
Dr. Ruth David	ANSER
Mr. Christopher Day	Private Consultant
Dr. William Delaney	Private Consultant
Ms. Lynn Dugle	Raytheon Company
Dr. Eric Evans	MIT Lincoln Laboratory
ADM William Fallon (ret)	Counter Tack, Inc
Dr. Craig Fields	Private Consultant
Dr. James Gosler	Johns Hopkins Univeristy Advanced Physics Laboratory
Mr. Alfred Grasso	MITRE
Hon. Paul Hoeper	Private Consultant
Dr. Miriam John	Private Consultant
Hon. Anita Jones	University of Virginia
Hon. Paul Kaminski	Technovation, Inc.
Dr. Ronald Kerber	Private Consultant
GEN Paul Kern (RET)	The Cohen Group
Hon. Donald Kerr	Private Consultant
Gen. Lester Lyles	Private Consultant
Dr. John Manferdelli	Intel
Dr. Joseph Markowitz	Private Consultant
Dr. Mark Maybury	MITRE
Hon. James Miller	Private Consultant
Hon. Judith Miller	Private Consultant
Mr. Robert Nesbit	Private Consultant
Maj. Gen. Paul Nielsen, USAF (ret)	Software Engineering Institute, Carnegie Mellon University

Mr. Michael Rich	RAND Corporation
Hon. William Schneider, Jr.	International Planning Services, Inc
Dr. Ralph Semmel	Johns Hopkins Univeristy Advanced Physics Laboratory
Mr. James Shields	Charles Stark Draper Laboratory
Mr. Robert Stein	Private Consultant
VADM Edward Straw	Private Consultant
Mr. David Van Buren	L-3 Communications
Mr. Lou Von Thaer	Leidos
Gen. Larry Welch	Institute for Defense Analyses
Dr. Robert Wisnieff	IBM

Government Advisers

Ms. Cathy Johnston	Defense Intelligence Agency
Dr. William LaPlante	U.S. Air Force

Defense Science Board Office

CAPT James CoBell	Deputy for Operations, US Navy
Lt. Col. Michael Harvey	Deputy for Operations, US Air Force
Ms. Janice Jackson	Defense Science Board
Mr. David Jakubek	Director, Defense Science Board Office
Ms. Debra Rose	Defense Science Board

Staff

Ms. Renée Bésanson	Strategic Analysis, Inc.
Mr. Brian Booth	Strategic Analysis, Inc.
Ms. Hannah Freeman	Strategic Analysis, Inc.
Mr. Marcus Hawkins	Strategic Analysis, Inc.
Dr. Toni Maréchaux	Strategic Analysis, Inc.
Ms. Mary Ellen Pascoe	Strategic Analysis, Inc.
Ms. Margaret Rowland	Strategic Analysis, Inc.
Ms. Jenifer Schimmenti	Strategic Analysis, Inc.
Ms. Stephanie Simonich	Strategic Analysis, Inc.
Ms. Jesse Strauss	Strategic Analysis, Inc.
Mr. Ted Stump	Strategic Analysis, Inc.
Mr. Zach VanSice	Strategic Analysis, Inc.